



# **Department of Veterans Affairs**

Employee Education System  
and  
Office of Cyber and Information Security

**presents**

# **VA Cyber Security Awareness**

**June 1, 2004**  
**Course ID:03.MN.SH.OCSWEB.A**  
**VA National Catalog Number: ITECH-EES-F249**

---

**Purpose:**

This program addresses key security practices and procedures for VA staff and incorporates the Office of Cyber and Information Security top initiatives that all VA employees, contractors and volunteers and all who access or utilize VA computers, networks and electronic information systems need to be aware of to protect VA's information assets. The Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) mandates that each federal agency provide annual training in computer security awareness.

**Outcome Objectives:**

Upon completion of this program participants will be able to:

1. describe the importance of identifying their Information Security Officer (ISO) and situations in which it is important to make contact with the facility or program ISO;
2. create passwords in a manner that maintain their security effectiveness;
3. recognize confidential information and handle in a manner consistent with VA Policy;
4. comply with cyber security requirements that protect an individual's privacy;
5. practice individual actions that ensure sensitive data is backed up;
6. recognize dangerous activities when using e-mail;
7. report suspected cyber security incidents to the ISO;
8. recognize that VA's information is an important part of the nation's critical infrastructure;
9. identify when an attempt is made to extract information without authorization;
10. identify instances where the use of VA's information resources is not authorized under the concept of "Limited Personal Use"; and
11. determine when computer equipment needs to be thoroughly "scrubbed"

**Target Audience:** This course is for all VA employees, contractors and volunteers and all who access or utilize VA computers, networks and electronic information systems.

**Content Area:** Information Resource Management

**Topic:** Security Awareness

**Lesson Outline:**

Introduction	Viruses
Know Your ISO	Incidents
Passwords	Infrastructure Protection
Confidentiality	Social Engineering
Privacy	Authorized Use
Backups	Post Test
Email	

## Welcome and Introduction

Welcome to the Veterans Affairs (VA) Office of Cyber and Information Security Awareness Training Course. The Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) mandates that each federal agency provide periodic training in computer security awareness and accepted computer practices for all employees, contractors, and volunteers. This training meets those requirements. The course is designed to take approximately 1 hour.

This course will help you to understand the responsibilities you have to protect VA's information assets, especially information about our veterans and it shows you ways to meet these responsibilities.

Successful completion of this course will fulfill your requirement for annual information security awareness training established under public law, VA policy, and other requirements.

### **PRIVACY STATEMENT** - Read before you continue with the course

This course is mandatory for all VA employees, contractors and volunteers and any persons that utilize VA computers, networks, and electronic information systems. This training is posted and refreshed annually. All new employees, contractors and volunteers are required to take this training within 30 days of joining VA.

A team of subject matter experts from the VA Office of Cyber and Information Security (OCIS) and VA Employee Education System (EES) created and developed this training.



"Cyber Security Awareness" is the knowledge that VA employees, contractors, and volunteers utilize to protect VA computer systems and data. It is more than policies, procedures, rules, and regulations. Cyber Security Awareness refers to the personal responsibility each of us assumes for ensuring:

- the confidentiality, integrity, and appropriate availability of veterans' private data,
- timely and uninterrupted flow of information throughout the VA enterprise, and
- VA information systems are protected from the potential of fraud, waste and abuse.

Please be aware of any activity that might violate and/or compromise the security of the VA information systems. Report all incidents to your information security officer.

## Know Your ISO

- Do you know all the rules and requirements you should follow to keep VA's information secure?
- Do you know what to do if your computer is infected with an electronic virus?
- If you witnessed someone using VA's computers for theft or fraud, what would you do?
- Do you know your responsibilities for maintaining confidentiality and privacy?
- Are you sure that your work is backed up and safe?
- Do you know your role in your facility's contingency plan?



There is someone available to help you - your facility Information Security Officer (ISO). Every VA facility has an assigned ISO who can help answer these questions and more.

It is important to know that we are all responsible for information security. Your ISO is a great resource for learning about those responsibilities and how to react if you become aware of a problem.

If you do not know your ISO, ask your supervisor.

**The ISO for the Dorn VAMC is  
Ms. Ava J. Ellis - extension 6383 or pager 769**

## Passwords

Passwords are important tools for getting your job done. They ensure you have access to the information you need. Keep your password secret to protect yourself and your work. If you have several passwords, it is permissible to record and store them in a safe place, to which only you have access.

## Password Requirements

Passwords must:

- Be constructed of at least eight characters (i.e., Gabc123&).
- Use at least three of the following four kinds of characters:
  - Upper case letters (ABC...)
  - Lower-case letters (...xyz)
  - Numbers (0123456789)
  - "Special characters," such as #, &, \*, or @.
- Be changed at least every 90 days. on all information systems.



Using these rules will provide you with a "strong" password. VA requires strong passwords.

## Password Theft

Passwords can be easily stolen or duplicated if constructed poorly. Most password thefts occur as a result of poorly constructed passwords or social engineering. We'll discuss social engineering later in this course.

## Poor Password Construction

Many factors can contribute to poor passwords. Some of the most notable are:

- Passwords that are not "strong," as explained above.
- Use of common words easily obtained from a dictionary.
- Passwords referring to your personal life (for example, names of family members or pets).

Easily identifiable passwords are an open invitation to hackers.

## Rules of Thumb for Passwords

- Don't use words found in a dictionary.
- Follow the rules for strong passwords.
- Don't use personal references (names, birthdays, addresses, etc.)
- Change your passwords at least every 90 days. If you suspect that someone is trying or may have obtained your password, change it immediately, and inform your information security officer.
- Be sure nobody can watch over your shoulder while you type your password. Ask them to turn away while you type. Position your keyboard so that it is not easy to see what you type.
- Keep passwords secret. Don't tape them to your computer, monitor, or keyboard. If due to the number of passwords you have to remember, you may want to write them down and you must securely lock them away where they cannot be accessed by others. Remember, don't store your passwords in the computer, as you may not be able to access them when you need them.
- Help to ensure that passwords and accounts for employees, volunteers, contractors, and students are terminated within 24 hours of their departure.



## Remembering Passwords

Since childhood, many people have used simple rhythms to remember things. Can you remember how you learned the alphabet, months of the year, state capitols, etc.? This is called using "mnemonics." For example, here is a mnemonic used to remember the planets of our solar system and their order is the rhythm:



**"Mary Very Easily Makes Jam Saturday Unless No Plums"**

Helps you to remember

**Mercury, Venus, Earth, Mars, Jupiter, Saturn,  
Uranus, Neptune, Pluto**

It may sound silly, but it works. Your memory makes sensible links between information, fitting facts into mental structures and frameworks. Building a simple mnemonic may not work if it does not make sense, but it only needs to make sense to you.

Mnemonics are a useful tool in constructing passwords that cannot be found in a dictionary. How about using this as a password for the mnemonic above:

**MVEMJS,unp**

For more information about passwords, ask your Information Security Officer (ISO).

## **Confidentiality**

In VA, confidentiality is a must. Perhaps you have wondered what this means and what you need to do about it. Confidentiality is the condition in which VA's information is available to only those people who need it to do their jobs.



Breaches in confidentiality can occur if you walk away from your computer without logging off or when paper documents are not adequately controlled. They sometimes occur when you are accidentally given access to too much computer information. Put another way, breaches can occur when someone has access to information that they do not need to do their jobs. Conversations about veteran's cases in public places such as elevators and hallways can be a breach of confidentiality.

VA's computers are designed to protect confidentiality, but remember that there are things you can do, and things you should not do, to protect confidentiality.

## **Computer Disposal and Confidentiality**



Getting rid of old computer equipment? Be careful! We in VA often look for ways to assist the community; it's one of the best things about us.

Not long ago, some VA computers containing patient data and other information were inadvertently released into the community. This created an unacceptable and very serious breach of confidentiality. Imagine seeing your own personal information on a used VA computer that was donated to a school! While it is usually the responsibility of Information Technology (IT) staff to ensure the complete erasure of data before disposal of equipment, there are things you can do to help.



- When possible, store your data on network drives instead of your desktop computer.
- If you notice computers being accessed without full data erasure, let your ISO know.
- Know that the "delete" command cannot remove all traces of data from your computer.

To address the problem of removing all data from computers prior to disposal, VA's Office of Cyber and Information Security has purchased a special software tool. This tool prepares computers for proper disposal by "overwriting" the data on a hard drive several times. This process obliterates and makes the data irretrievable in any form. Every VA facility has received this tool for the IT staff to use. Working together, we will ensure that this never happens again!

Your ISO can help you find other ways to secure your data. For more information, contact your facility Information Security Officer (ISO).

## Privacy



As Americans, we have fundamental expectations for privacy. The right to privacy is even built into our Bill of Rights as a basic human dignity afforded citizens.

Privacy has a special legal meaning for government agencies. The Privacy Act requires that we as government employees take special care when we provide information to anyone about our veterans and other customers. Providing personal information to anyone, including veterans themselves, must be done only by persons authorized to do so. The same applies to requesting and receiving information about ourselves as employees and/or as veterans. Care must also be taken to assure that recipients of information are authorized to receive that information. As VA employees, we must follow legal procedures for giving out and receiving information. These procedures ensure that information is distributed in a responsible manner and that VA accounts for the transaction.

## Information Privacy, Security, and the VA Mission

Part of the VA mission is to ensure America's veterans receive medical care and benefits with dignity and compassion. To accomplish this, VA gathers all kinds of information from and about its beneficiaries. Much of it is related to health care, military service, finances, education, and other personal information. Lest we forget, something as simple as a veteran's home address and phone number is privileged information. The Privacy Act requires that we as government employees take special care when we provide information to anyone about veterans and others. The Healthcare Insurance Portability and Accountability Act (HIPAA), is an additional requirement with which VA must comply. HIPAA established federal criminal penalties for wrongfully using/disclosing protected health information. If you handle health care information in your job at VA, you need to know about HIPAA. HIPAA grants rights to individuals and imposes obligations on organizations. For more information on Privacy and HIPAA you can go to the Privacy Awareness course or contact your local Privacy Officer.



## Helpful Guidance for Handling Privacy Requests

If another VA employee asks you for veteran information under your control, your response may depend on several things, including:

- The purpose of the request
- The authority of the individual making the request
- The established procedures for managing the request.

If the request does not follow the standard procedures that you are familiar with, do not hesitate to consult your supervisor for directions prior to accessing or disclosing any information.

## A Little Curiosity Can Be Harmful...

...Don't let it hurt you, any veteran, or your coworkers.

It is human nature to be curious. We all may have occasional urges to find out a little bit more about each other. When tempted to delve into personal information about veterans you come in contact with or employees you work with, the best advice is stop and consider your actions:

- Do you have a need to know in order to do your job?
- The person you are curious about has the right to be treated with respect, dignity, and have their privacy maintained.
- Unauthorized access or use of veteran, employee, or enterprise information entrusted to VA is a serious offense. Disciplinary action can be brought against you as well as legal action that could result in civil and felony punishment.
-



Through established policies and procedures, VA has developed measures to protect the privacy and confidentiality of veterans and employees. Policies and procedures are only as good as the individuals who implement and follow them. Your informed knowledge and professional experience is the best defense against unauthorized use and disclosure of information.



Requests for information from the public, media (newspapers, or radio and television stations), and others must be handled in a manner that protects the privacy of veterans, their families, and confidential corporate information. Such requests must be referred to the appropriate official at your facility.

If you have questions about privacy in VA and your responsibilities as an employee, contact your supervisor, Privacy Act Officer, or Information Security Officer (ISO).

## Backups



The work you do on VA's computers is important. It is important to you because you spent time and effort to create it. It is important to VA and to veterans because it supports our mission.

Is your work "backed up" and safe from loss? In most VA facilities, systems managers have created ways to ensure your work is saved in several places (backed up) so it is not lost. You should make sure your work is backed up.



Making a copy of files for the purpose of having them available in case of a computer failure is called "backing up" or "creating a backup." Backups are done to a second storage medium such as a diskette, zip disk, CD, or tape. Information systems managers take purposeful steps to ensure that VA data is safe by systematically and routinely creating database backups on systems such as Vista, BDN, and others. It may not be reasonable to expect IT staff to be responsible for backing up the information on the computers of every user in your facility, so you may need to assume this responsibility yourself. If you are at all unsure if your work is backed up, contact your ISO.

Helpful suggestions to assist you in backing up your files:

- The most important files to backup are the ones you create such as word processing, spreadsheet, and presentation files. At home, you will want to back up your financial files (Quicken, Money, TurboTax, etc.).
- Software programs do not need to be backed up. They can usually be reinstalled from the original media.
- Store the files you create in a single location on your computer such as the "My Documents" folder. Doing so will make it easier to quickly create your backup. If you store your files in many different locations, it will be more time consuming to locate them and may prevent you from routinely backing

- up all of your files.
- Set a schedule for backups appropriate to your needs. Some people may need to create daily backups. For others, weekly or even monthly may be adequate. Don't risk any more data to inadequate backups than you are willing to lose or have to recreate.
- After creating a backup, verify that you can access your storage medium and open the files on it.
- Storage media wear out, especially magnetic media. It is like watching an old movie on film or videotape. The recorded signal gradually wears out resulting in a grainy or unstable picture. This happens over time. Rotate your storage disks and periodically replace them with new disks or new technology.
- Clearly identify the files on your storage medium. Trying to find a specific file in a pile of unlabeled disks is time-consuming and risky.
- Store your backups in a safe and secure place.



The most reliable computers are apt to eventually fail as a result of age, heat, dust, or mechanical failure.

Backups are cheap insurance. The question is not if you will ever need to use your backup. Instead, the question is when.

Ask your supervisor or Information Security Officer (ISO). They can tell you if your work is safe and can help you create a way to routinely back it up.

## Email

In VA, e-mail has become a vital tool in conducting our business. Proper use of VA electronic mail is essential to ensure this resource is uninterrupted and used in legal ways. Chain letters and hoax messages rob us of valuable network capacity, computer space, and processing speed. You should not forward these messages to others. In fact, don't even request the sender stop sending you messages. Just delete them. These "please stop" messages sent by the thousands slow down our e-mail systems! Sensitive information should not be sent using e-mail unless it can be done securely. Before you send sensitive information on e-mail, you must ensure that it can be done securely. Some computer viruses attack e-mail systems, making them unavailable. the signs of a virus infection.



## E-mail Privacy and Security

Do not think of e-mail as being similar to a personal letter delivered to you in a sealed envelope by the post office. Instead, e-mail is more like a postcard. Most often, it gets dependably delivered but there may be opportunities along the way for people other than the addressee to view the

contents.

E-mail is not considered private. You should have no expectation of privacy when using e-mail to transmit, store and communicate information.

E-mail is not considered secure. E-mail systems, including VA's, are vulnerable to virus attacks. In fact, most computer viruses are spread through e-mail messages.

### **E-mail hints for work and home.**

- Utilize virus-scanning software. Be sure it is kept up-to-date. Scan all e-mails and attachments sent to you.
- Always be cautious in opening e-mail from people you don't know. Make sure the subject lines are appropriate before opening. If you are not sure whether the e-mail is legitimate, then contact the sender by phone.
- Don't open attachments from people you don't know.
- Utilize e-mail in an appropriate manner. Don't forward or create hoaxes or ask people to modify their computer systems. Don't spread rumors using e-mail. Be suspicious of any message that tells you to forward it to others.
- Unsubscribe from mailing lists in which you are no longer interested.
- Don't participate in "mail-storms" involving scores (or hundreds or even thousands) of users responding "me too!" or "thanks" or even "please stop."
- Use "reply to all" sparingly. Does everyone in your large mail group really need to see your response? Often, it is more appropriate to limit your response to just the sender.



Where do you go for information about the security or e-mail, questionable, improper, or illegal e-mail messages? You should consult your supervisor or local Information Security Officer (ISO) to ensure that VA e-mail is being used properly and securely or if you have questions about these issues.

### **Viruses**



Do you know that computer viruses can be one of the biggest causes of business loss in VA? High-tech vandals have created ever-more dangerous infectious programs that, in the past, have overcome VA's defenses. When that happens the data we depend on to fulfill our mission is compromised. It takes time and money to defend against viruses. It requires employee time to recover from attacks. Viruses make our jobs more difficult and steal resources away from our primary mission of serving veterans. Take an active role in virus defense. Find out if the computer you are

using is protected. When antivirus programs are loading, let them run to completion. Be suspicious of e-mail messages from people you do not know as well as of unexpected messages from people you do know. Look for suspicious activity, like a constantly active hard drive. Make sure data files and programs you load on your computer are authorized and free from viruses.

Improvements in technology have permitted VA to institute an enterprise-wide anti-virus defense program. Often, anti-virus software is automatically installed and updated. Nonetheless, new viruses are an everyday occurrence, and antivirus software offers no

protection from newly developed, unknown viruses. Viruses can be spread from inside as well as from outside VA. Learn how tell if the antivirus programs on your work and home computers are running and current.

## **Worms and Trojan Horses**

Software specifically designed to damage, corrupt, and disrupt a computer or network system is collectively known as malicious software, or "malware." It may be called a virus or worm and be carried by a Trojan horse. Here are some basic definitions for types of malware and how they impact your system.

A virus is a software program loaded onto your computer and executed without your knowledge.

One type of virus is called a worm. Worms can replicate themselves. A simple virus that can make a copy of itself over and over again is relatively easy to produce. A worm can be dangerous because it quickly uses all the available memory of your system and bring it to a halt. Viruses capable of transmitting themselves across the network and bypassing VA protections are even more dangerous because they infect system after system within the VA.



Another type of virus is called a "Trojan Horse." The term Trojan Horse comes from a story in Homer's Iliad, in which ancient Greeks give a giant wooden horse to their foes, the Trojans, as a peace offering. After the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in, capture and destroy the city of Troy. As the name implies, these destructive programs masquerade as benign applications. Trojan Horses do not replicate themselves but they can be just as destructive. Their mission is to carry destructive viruses and introduce them into your computer or network. One of the most insidious types of Trojan Horse programs is one that claims to rid your computer of viruses but instead introduces viruses onto your computer.



Viruses can be contracted through a variety of access points on your computer, from a software diskette, a CD-ROM, DVD, removable storage medium (zip drives, etc.) or e-mail.

Malicious e-mail hoaxes are not viruses, but they are also potentially dangerous. In most cases, the sender asks you to forward a warning message "to everyone you know." The hoax may request the recipient to take corrective action, which instead, disables your system. A good example of an e-mail hoax is one that has a subject line: "Delete this file immediately." The message provides instructions on how to locate a critical computer system file and delete it. Even seemingly well-intentioned messages, when forwarded by thousands of recipients to thousands more recipients are bad because they slow down the entire VA network. In turn, this delays our important work of serving America's veterans.

## **Symptoms**

If your computer has any of these symptoms, there may be a problem.

Your computer:



- reacts slower than usual.
- stops running for no apparent reason.
- fails to boot.
- seems to be missing important files.
- prevents you from saving your work.



## **Virus defense for work and home**



In VA, all computers are required to have virus protection software. To be effective, the virus protection software must be kept up to date. New updates are usually issued every week. Contact your ISO or information technology staff if your VA computer is not up to date. While many sites automatically update virus protection software on networked computers, remember that non-networked computers, particularly VA issued laptops, will not receive automatic updates to virus protection software. If your computer is not networked it is particularly important that you assure that the virus protection software is regularly updated.

Here is a list of things you can do:

- Delete e-mail messages with unusual subject lines, for example, "Open this immediately."
- Never stop or disable your anti-virus program.
- Always allow an anti-virus program to perform its routines without interruption.
- Back up your files on a regular schedule.
- Have your virus protection software set to scan your e-mails and attachments.
- Be cautious and sensitive to attachments that have file extensions that execute system commands or applications. For example: .exe, .vbs, .js, .jse, .wsf, .vbe and .wsh.
- Unless you can verify, do not delete any system files based on a request made on e-mail.

To learn more about computer viruses and your role in virus defense, talk to your Information Security Officer (ISO).

## **Incidents**



Take a few moments to consider how important VA's computers are in conducting our business. Almost everything we do depends on our computers. Unfortunately, the same computers that help us serve veterans can also be used for theft and fraud. Electronic viruses can attack our computers. They can be stolen and vandalized. They can be used to distribute sensitive information to those not authorized to receive it. All these are examples of computer-related incidents. It is important to let your supervisor and Information Security Officer (ISO) know when you witness such incidents. Your ISO will contact the VA

Central Incident Response Capability (VACIRC). Reporting cyber security incidents helps VA to reduce the negative impact of these events and to improve VA's information processing ability.

VACIRC was established to fulfill VA's need to ensure that computer security incidents are detected, reported and corrected as quickly as possible, and with minimal impact. VACIRC's primary responsibilities are to:

- Serve as a central clearinghouse for all reported incidents, security alerts, and notifications;
- Ensure additional CIRC resources for all VA incidents as needed;
- Coordinate effective notification of and response to all reported incidents;
- Notify proper officials in each organization of reported incidents.

## Incident Do's and Don'ts

When you think a computer security incident may have occurred, you should



- Gather details of the incident so you can communicate specific information to your ISO.
- Collect the date, time, location, and involved computer systems.
- Describe what you believe happened.
- Write down any error messages displayed on your computer screen.
- Write down any involved web addresses, server names, or IP addresses.

Time may be of the essence. Don't wait to call your ISO.

E-mail may not be the best way to report the incident. You may need to contact your ISO by phone or in person.

Limit discussion of the incident to only those with a specific need to know.

Do not discuss the incident with the media (radio, TV, newspapers) or anyone outside of your facility without first consulting your ISO and facility management.



To report a cyber security problem, your primary point of contact is your information security officer. To learn more about VACIRC, visit their web site at [vacirc.va.gov](http://vacirc.va.gov).

## VA Cyber Security: Part of Infrastructure Protection



As a VA employee, you must be aware that the Department's information systems are part of America's strategic infrastructure. We are expected to maintain our ability to provide veteran services even in times of national tension. VA's information systems not only enable us to provide efficient services to America's veterans, they also enable VA to work with other agencies, including the Departments of Defense (DoD), Health and Human Services (HHS), and Homeland Security. In addition to our primary mission of

serving veterans, VA has a role in responding to a variety of regional and national emergencies.

The FBI has warned all Federal agencies that their systems and the information in those systems are potential targets for an ever-increasing number of cyber attacks. Now more than ever, the VA's systems and the information they contain must be available to serve our nation and its veterans. Please be alert to anything that might compromise VA's cyber security. Immediately report any incidents to your Information Security Officer. If your ISO is unavailable, contact VACIRC at 1-877-279-8856.



Contact your facility Information Security Officer (ISO) if you have questions about cyber security issues. For general information about VA's Cyber Security program, go to [vawww.infosec.va.gov](http://vawww.infosec.va.gov).

## Social Engineering



Have you heard of "social engineering?" Social engineering is an unauthorized person's manipulation of your trust to get you to give up information or resources that you should not give out. This is an important information security issue!

Make sure when you are asked by someone to provide information or allow the use of your computer or accounts (in person, over the phone, or electronically), that you are certain of who they are and of their authorization to have/use that information or access as part of their job. Dishonest "social engineers" look for almost any kind of information to misuse, like your password or patient, budget, or employee information. VA employees have a natural desire to be helpful and provide useful information. Social Engineers try to take advantage of this to misuse resources or information.



One example of social engineering perpetrated on VA facilities comes in the form of a phone call from someone claiming to be from "the phone company." The thief says they are testing lines and long distance circuits and instructs the employee to dial a special code that gives the caller access to FTS long distance service. This scam has resulted in thousands of dollars worth of unauthorized calls being made at VA expense.

Unauthorized disclosure of information or granting of resources to dishonest social engineers are potentially bigger threats to you and VA than most computer hackers. To learn more about social engineering and your role in defending against it, contact your Information Security Officer (ISO).



## Authorized Use

The citizens of our country expect that as VA employees, we will not misuse or abuse the resources provided to us to accomplish our mission. As a VA employee, you may have the privilege of some "Limited Personal Use" of certain government resources, such as computers, e-mail, Internet access, and telephone/fax service. This benefit is available only as long as it does not interfere with official VA business, involves minimal additional expense to the Government, and is legal and ethical. Remember that your personal use may be limited at any time either by your management or by those responsible for the particular government resource you want to use. Before using this privilege, you should discuss your limits and responsibilities in using it with your supervisor and Information Security Officer (ISO).



## Ethics

"Ethics is about understanding how your actions affect other people, knowing what is right and wrong, and taking personal responsibility for your actions..."

- Winn Schwartau

- **Ethics** deals with placing a "**value**" on acts according to whether they are "**good**" or "**bad**." Every society has its rules about whether certain acts are ethical or not. The same thing is true when using a VA computer system to access confidential information.

## Misuse or Inappropriate Use

Examples of Misuse or Inappropriate Use includes the following:

- Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, continuous data streams, video, sound, or other large file attachments that degrade performance of VA's network.
- Using VA systems as a staging ground or platform to gain unauthorized access to other systems.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
- The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any illegal activities or activities otherwise prohibited.
- Use for commercial purposes or in support of "for profit" activities or in support of other outside employment or business activity (e.g. consulting for



pay, sales or administration of business transactions, sale of goods or services).

- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- Posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a VA employee (unless appropriate approval has been obtained), or uses that are at odds with the agency's mission or positions.
- Any use that could generate more than minimal additional expense to the government.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information; copyrighted, trademarked, or material with other intellectual property rights beyond fair use; proprietary data; or export-controlled software or data.



Be sure to discuss your limits and responsibilities with your supervisor and Information Security Officer (ISO).

To receive credit for this course, you must complete and return the attached post-test to Education Service Line (141)



# VHA Cyber Security Training POST TEST

To receive credit for this course, you must complete  
and return this test to Education Service Line (141)

NAME \_\_\_\_\_ LAST 4 OF SSN \_\_\_\_\_  
DATE \_\_\_\_\_

**1. If you think your workstation has been infested with a virus, you would contact:**

- a. Your computer manufacturer.
- b. Your Information Security Officer (ISO).
- c. Norton Virus Protection, Inc.
- d. Your Service Chief.
- e. None of the above.

**2. Which of the following Rules of Thumb for passwords do not apply:**

- a. Do not use words found in any dictionary.
- b. Do not use personal references (for example: names, birthdays, addresses).
- c. Have your friend keep a copy of your password in case you forget.
- d. Keep passwords secret.
- e. Follow the rules for creating good, strong passwords.

**3. Hitting the Delete key on your computer will erase the information from your computer completely.**

- a. True
- b. False

**4. What is one of the major purposes of HIPAA?**

- a. Provides information about privacy to the veteran audience.
- b. Outlines privacy policies and procedures for VA employees.
- c. Clarifies and standardizes responsibilities government employees have regarding providing information about veterans.
- d. Clarifies the privacy guidelines mandated by all health insurance companies.

**5. What is a backup?**

- a. Keeping your supervisor and coworkers informed about where you keep important documents and files.
- b. Routinely copying your computer and email files to a second storage medium.
- c. Creating duplications of important files and documents for storage with the originals.
- d. Informing your ISO every time you or your team create an important document.

**6. What should you do if you receive an email attachment from someone you don't know?**

- a. Do not open the attachment.
- b. Open the attachment if the subject line seems appropriate.
- c. Reply to the email and request more information.
- d. Open the attachment if your virus software doesn't alert you not to.

**7. Software specifically designed to damage, corrupt, and disrupt a computer or network system is collectively known as:**

- a. Computer destroyer
- b. Malicious software, or "malware"
- c. Junk mail
- d. Spam

**8. When you think a computer security incident may have occurred, you should:**

- a. Gather details of the incident so you can communicate specific information to your ISO.
- b. Collect the date, time, location, and involved computer systems.
- c. Describe what you believe happened.
- d. Write down any error messages displayed on your computer screen.
- e. Write down any involved web addresses, server names, or IP addresses.
- f. None of the above
- g. All of the above.

**9. VA information systems enable the Department to work with other agencies, including Department of Defense (DoD), Health and Human Services (HHS), and Homeland Security during times of national tension.**

- a. True
- b. False

**10. The citizens of our country expect that as VA employees, we will not misuse or abuse the resources provided to us to accomplish our mission.**

- a. True
- b. False

**11. Social Engineering is an unauthorized person's manipulation of your trust to get you to give up information or resources that you should not give out.**

- a. True
- b. False

**12. As a VA employee, you may have the privilege of some "Unlimited Personal Use" of certain government resources, such as computers, e-mail, Internet access, and telephone/fax service.**

- a. True
- b. False

**13. Which statement best represents the definition of confidentiality in the VA?**

- a. Confidentiality is the condition in which VA's information is available to only those people who need it to do their jobs.
- b. Confidentiality is the condition in which information whose unauthorized disclosure could be prejudicial to the national interest.
- c. Confidentiality is a feeling or consciousness of one's powers or of reliance on one's circumstances.

**14. In the VA, passwords must:**

- a. Have a minimum of eight characters.
- b. Be changed every 120 days.
- c. Include your middle initial.
- d. Have all letters capitalized.

**15. Which is not an example of how a social engineer may gain your trust to get unauthorized information:**

- a. You receive an e-mail message from your new computer service technician asking for your username and password.
- b. You receive a phone call from the telephone company technician who needs your username and password in order to complete their testing of the phone lines in your facility.
- c. You receive a letter from the friend of a veteran asking for important medical information.
- d. You receive a call telling you that they want to break into your computer system.